View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Elsevier - Publisher Connector

JOURNAL OF NUMBER THEORY 29, 251–263 (1988)

Remarks on Exponential Congruences and Powerful Numbers

P. RIBENBOIM

Department of Mathematics and Statistics, Queen's University, Kingston, Ontario K7L 3N6

Communicated by Hans Zassenhaus

Received December 2, 1986; revised January 29, 1987

The study of Fermat's last theorem (FLT) has led, among other things, to the consideration of exponential congruences and powerful numbers (the natural numbers n, such that if p is any prime which divides n, then p^2 divides n).

Namely, if p is an odd prime and if there exist integers x, y, z, not multiples of p, such that $x^p + y^p = z^p$ (i.e., the first case of FLT is false for p), then $2^{p-1} \equiv 1 \pmod{p^2}$, and more generally $l^{p-1} \equiv 1 \pmod{p^2}$ for every prime $l \leqslant 89$ (see [12, 5]).

Quite recently, Granville [4] showed that if there do not exist three consecutive powerful numbers, then the first case of FLT is true for infinitely many primes p.

The purpose of this note is to elaborate on the connection between exponential congruences, powerful numbers, and Fermat's last theorem.

The tools will be certain results about Catalan's equation, as well as theorems of Schinzel and Tijdeman, based on Baker's method. It is convenient to state these facts explicitly:

(A) Gerono [13]: If l is a prime and $m \geqslant 2$ then $l^m + 1$ is not a proper power (square, cube, etc...).

(B) Lebesgue [13]: If $a \geqslant 2$ then $a^2 + 1$ is not a proper power.

(C) Euler, Chao Ko [13]: If $a^2 - 1$ is a cube, then $a = 3$; if $a \geqslant 2$ then $a^2 - 1$ is not a kth power, when $k \geqslant 4$.

(D) Nagell [9]: If $a \geqslant 3$ then $a^3 \pm 1$ is not a proper power.

(E) Ljunggren [7]: If $x \neq 0, \pm 1$, $n \not\equiv -1 \pmod 6$ and if there exists $y \geqslant 1$ such that $(x^n - 1)/(x - 1) = y^3$ then $n = 3$, $x = 18$ or -19, $y = 7$.

0022-314X/88 $3.00

Copyright © 1988 by Academic Press, Inc.
All rights of reproduction in any form reserved.

(F) Tijdeman [18]: There exists an effectively computable constant $C_1 > 0$, such that if x, y, z, t are integers, $x, y \geqslant 1$, $z, t \geqslant 2$, and $x^z - y^t = 1$, then $x, y, z, t \leqslant C_1$.

(G) Schinzel and Tijdeman [17]: Let $f(X) \in \mathbb{Q}[X]$, with at least two distinct roots. Then there exists an effectively computable constant $C = C(f) > 0$, such that if x, y, z are integers, $|y| \geqslant 2$, $z \geqslant 1$, and $f(x) = y^z$, then $z \leqslant C$.

(H) Schinzel and Tijdeman [17]: Let $f(X) \in \mathbb{Q}[X]$, with at least two simple roots. Then there exists an effectively computable constant $C = C(f) > 0$, such that if x, y, z are integers, $|y| \geqslant 2$, $z \geqslant 3$, and $f(x) = y^z$, then $x, y, z \leqslant C$.

(I) Schinzel and Tijdeman [17]: Let $f(X) \in \mathbb{Q}[X]$, with at least three simple roots. Then there exists an effectively computable constant $C = C(f) > 0$, such that if x, y, z are integers, $|y| \geqslant 2$, $z \geqslant 2$, and $f(x) = y^z$, then $x, y, z \leqslant C$.

1. Exponential Congruences and the First Case of FLT

According to the theorems of Wieferich, Mirimanoff, Vandiver, Pollaczek, Morishima, Granville, and Monagan, *if the first case of* FLT *is false for p then*

$$l^{p-1} \equiv 1 \pmod{p^2}$$

for every prime $l \leqslant 89$.

Since $2^{p-1} \not\equiv 1 \pmod{p^2}$ for $p < 6 \times 10^9$ (except for $p = 1093$ and 3511) and $3^{p-1} \not\equiv 1 \pmod{p^2}$ for $p = 1093$ and 3511, then *the first case of* FLT *is true for every* $p < 6 + 10^9$. Even better, it holds for $p < 714{,}591{,}416{,}091{,}389$, as follows from the combination of the above criteria, using Gunderson's method [6].

From Wieferich's criterion, it is immediate [11] that *the first case of* FLT *holds for every Mersenne prime number* $p = M_q = 2^q - 1$ (q prime); for example, *it holds for* M_{216091}, *which is the largest prime known today.*

Similarly, if $L > 1$ let $\mathcal{N}_L = \{p \text{ prime} \mid \text{there exists } c \leqslant 1,\ p \nmid c, \text{ such that } pc = u \pm v, \text{ with every prime factor of } uv \text{ at most equal to } L\}$.

It is also easy to see that *if* $p \in \mathcal{N}_{89}$ *then the first case of* FLT *is true for p.*

Adleman, Heath-Brown, and Fouvry combined their efforts to prove [1, 3] that *the first case of* FLT *is true for infinitely many primes.* This was established appealing to very fine and difficult new results in sieve theory. It is natural to ask whether the same result may be achieved by other means—but this remains to be seen. Anyway, some possible paths will be

proposed below; at present, they appear to be at least as difficult as Fouvry's approach.

For $k \geqslant 1$ and any prime $l \geqslant 2$, let $\mathscr{W}_l^{(k)} = \{p \text{ prime} \mid l^{p-1} \equiv 1 \pmod{p^k}\}$.

Thus $\mathscr{W}_l^{(1)}$ is the set of all primes different from l.

Heuristically, the probability for the existence of a prime $p \leqslant x$ such that $l^{p-1} \equiv 1 \pmod{p^2}$ is equal to

$$\sum_{p \leqslant x} \frac{1}{p} = \log\log x + O(1).$$

So, for every $l \geqslant 2$, the set $\mathscr{W}_l^{(2)}$ should be infinite. On the other hand, if $k \geqslant 3$ the probability for a prime $p \leqslant x$ to satisfy $l^{p-1} \equiv 1 \pmod{p^k}$ is at most equal to $\sum_{p \leqslant x} (1/p^{k-1}) < \zeta(k-1) < \infty$.

Thus, the sets $\mathscr{W}_l^{(k)}$ (with $k \geqslant 3$) should be finite.

Now, for every $l \geqslant 2$ and $k \geqslant 1$, let $\mathscr{N}_l^{(k)} = \{p \text{ prime} \mid \text{there exists } s \geqslant 1$ such that $1 \leqslant v_p(l^s + 1) \leqslant k\}$ (where v_p denotes the p-adic valuation).

Clearly $\mathscr{N}_l^{(1)} \subseteq \mathscr{N}_l^{(2)} \subseteq \mathscr{N}_l^{(3)} \subseteq \cdots$ and $\bigcup_{l \leqslant 89} \mathscr{N}_l^{(1)} \subseteq \mathscr{N}_{89}$.

In view of a result quoted above, if there exists a prime $l \leqslant 89$ such that $\mathscr{N}_l^{(1)}$ is infinite, then the first case of FLT is true for infinitely many primes. Up to now, it is not known whether $\mathscr{N}_l^{(1)}$ is infinite (for any prime l). In 1968, in a rather unnoticed paper, Puccioni [11] showed that *if l is a prime, $l \not\equiv \pm 1 \pmod 8$, then $\mathscr{N}_l^{(1)} \cup \mathscr{W}_l^{(3)}$ is an infinite set.* Heuristically, $\mathscr{W}_l^{(3)}$ is a finite set (up to now, no number in $\mathscr{W}_2^{(3)}$ is known), thus $\mathscr{N}_l^{(1)}$ is heuristically infinite.

The following proposition contains the result of Puccioni, with a modification of his proof:

PROPOSITION 1. *For every $k \geqslant 1$ and prime $l \geqslant 2$:*

(1) $\mathscr{N}_l^{(k)} \cap \mathscr{W}_l^{(k+1)} = \begin{cases} \varnothing & \text{if } l \not\equiv 1 \pmod{2^{k+1}}, \\ \{2\} & \text{if } l \equiv 1 \pmod{2^{k+1}}, \end{cases}$

(2) $\mathscr{N}_l^{(k)} \cup \mathscr{W}_l^{(k+2)}$ *is an infinite set.*

Proof. (1) First, it will be shown, by induction on k, that $\mathscr{N}_l^{(k)} \cap \mathscr{W}_l^{(k+1)} \subseteq \{2\}$.

If $k = 1$ and p is an odd prime such that $p \in \mathscr{N}_l^{(1)} \cap \mathscr{W}_l^{(2)}$, then $l^{p-1} \equiv 1 \pmod{p^2}$ and there exist $s \geqslant 1$, $c \geqslant 1$, such that $p \nmid c$, $l^s + 1 = pc$; since $l^p \equiv l \pmod{p^2}$ then $l^s \equiv l^{ps} = (pc-1)^p \equiv -1 \pmod{p^2}$, so $p^2 \mid l^s + 1$, which is absurd.

Assume the statement true for $k \geqslant 1$. First note that $\mathscr{N}_l^{(k)} \cap \mathscr{W}_l^{(k+2)} \subseteq \mathscr{N}_l^{(k)} \cap \mathscr{W}_l^{(k+1)} \subseteq \{2\}$. It suffices to show that $(\mathscr{N}_l^{(k+1)} \setminus \mathscr{N}_l^{(k)}) \cap$

$\mathscr{W}_l^{(k+1)} = \varnothing$. Let p be a prime in this set, so $l^{p-1} \equiv 1 \pmod{p^{k+2}}$ and there exists $s \geqslant 1$, $c \geqslant 1$, such that $p \nmid c$, $l^s + 1 = p^{k+1}c$; since $l^p \equiv l \pmod{p^{k+2}}$ then $l^s \equiv l^{ps} \equiv (p^{k+1}c - 1)^p \pmod{p^{k+2}}$. If $p \neq 2$ then $l^s \equiv -1 \pmod{p^{k+2}}$, which is absurd. If $p = 2$ then $l^s \equiv 1 \pmod{2^{k+2}}$ and $2^{k+1}c \equiv l^s + 1 \equiv 2 \pmod{2^{k+2}}$, hence $k+1 = 1$ and $k = 0$, which is absurd.

This shows that $\mathscr{N}_l^{(k)} \cap \mathscr{W}_l^{(k+1)} \subseteq \{2\}$.

Finally, if $2 \in \mathscr{N}_l^{(k)} \cap \mathscr{W}_l^{(k+1)}$ then $l \equiv 1 \pmod{2^{k+1}}$.

Conversely, if $l \equiv 1 \pmod{2^{k+1}}$ then $2 \in \mathscr{W}_l^{(k+1)}$ and $l + 1 \equiv 2 \pmod{2^{k+1}}$, so $2 \in \mathscr{N}_l^{(1)} \subseteq \mathscr{N}_l^{(k)}$.

(2) In this proof, (G) will be used and for the polynomial $f(X) = 2X^{k+1} - 1$, let C be the corresponding effectively computable constant.

If $\mathscr{N}_l^{(k)} \cup \mathscr{W}_l^{(k+2)}$ is assumed to be finite, let m be a prime number such that $m > C$ and $m > \max\{p \mid p \in \mathscr{N}_l^{(k)} \cup \mathscr{W}_l^{(k+2)}\}$. Let $P = \prod_{l \neq q \leqslant m} q$ (each factor q being a prime number). Hence $\phi(P) = \prod_{l \neq q \leqslant m} (q-1)$ and so, $\phi(P)$ is even and greater than C.

It is clear that $l^{\phi(P)} \equiv 1 \pmod{P}$. Also, if $q \neq 2$ and q divides $l^{\phi(P)} + 1$ then $q > m$—otherwise, $l \neq q \leqslant m$, so q divides P, hence $l^{\phi(P)} - 1$ and $q = 2$.

By the result of Gerono, stated in (A), $l^{\phi(P)} + 1$ is not a proper power.

First case. There exists a prime q such that q^{k+2} divides $l^{\phi(P)} + 1$.

If $q = 2$ then l is odd and $l^{\phi(P)} \equiv -1 \pmod 8$. But $l^2 \equiv 1 \pmod 8$ and $l^{\phi(P)} \equiv 1 \pmod 8$, which is absurd.

So $q \neq 2$, hence $q > m$, therefore $q \nmid \phi(P)$.

Let g be the order of l modulo q, hence g divides $q - 1$. But $q \mid l^{2\phi(P)} - 1$, so $g \mid 2\phi(P)$, and therefore $2\phi(P) = gh$, with q not dividing h.

Since q^{k+2} divides $l^{gh} - 1 = (l^g - 1)(l^{g(h-1)} + l^{g(h-2)} + \cdots + l^g + 1)$, and $l^g \equiv 1 \pmod q$, then the second factor above is congruent to $h \not\equiv 0 \pmod q$. Therefore q^{k+2} divides $l^g - 1$. So $l^{q-1} \equiv 1 \pmod{q^{k+2}}$, that is $q \in \mathscr{W}_l^{(k+2)}$ and hence, $q < m$, which is a contradiction.

Second case. If q divides $l^{\phi(P)} + 1$ then q^{k+2} does not divide $l^{\phi(P)} + 1$.

Since $l^{\phi(P)} + 1$ is not a $(k+1)$th power, there exists a prime q such that $q \mid l^{\phi(P)} + 1$, but $q^{k+1} \nmid l^{\phi(P)} + 1$. Hence $q \in \mathscr{N}_l^{(k)}$ and $q \leqslant m$. This implies that $q = 2$, so $l^{\phi(P)} + 1 = 2^e t^{k+1}$, where $1 \leqslant e \leqslant k$ and t is odd. But l is odd and $\phi(P)$ is even, so $l^{\phi(P)} \equiv 1 \pmod 4$, hence $e = 1$, that is $l^{\phi(P)} + 1 = 2t^{k+1}$.

Thus, the integers $t, l \neq 0$, $\phi(P) \geqslant 1$ are solutions of the equaton $2X^{k+1} - 1 = Y^Z$. Hence $\phi(P) \leqslant C$, which is an absurdity. ∎

The following question is open: do there exist infinitely many primes l such that $l^{p-1} \not\equiv 1 \pmod{p^2}$? In other words, is $\mathscr{W}_l^{(1)} \setminus \mathscr{W}_l^{(2)}$ an infinite set?

In this respect, Powell showed [14] that $\bigcup_{k \text{ odd}} (\mathscr{W}_l^{(k)} \setminus \mathscr{W}_l^{(k+1)})$ is an infinite set. Thus, heuristically, $(\mathscr{W}_l^{(1)} \setminus \mathscr{W}_l^{(2)})$ should be an infinite set.

2. Powerful Numbers and the First Case of FLT

A natural number n is *powerful* whenever: if p is any prime dividing n, then p^2 divides n.

It is easy to see that n is powerful if and only if it may be written in the form $n = a^2b^3$ (where $a, b \geq 1$); moreover, if b is squarefree, the representation is unique.

My recent expository paper, "Impuissants devant les puissances" [15], deals with some of the questions being studied in relation with powerful numbers. Here, the main concern is a conjecture of Erdös [2], which was repeated, unknowingly, by Mollin and Walsh [8]:

(E) There do not exist three consecutive powerful numbers.

Mollin and Walsh showed that *each of the following conditions is equivalent to the conjecture* (E):

(E_0) If a, b are powerful numbers, a is even and b is odd, then $a^2 - b \neq 1$.

(E_0') If $m > 0$ is squarefree and $m \equiv 7 \pmod 8$, if $t_1 + u_1\sqrt{m}$ is the fundamental unit of $\mathbb{Q}(\sqrt{m})$, if $t_k + u_k\sqrt{m} = (t_1 + u_1\sqrt{m})^k$ for $k \geq 1$, and if t_k is even and powerful, for some odd k, then either u_k is even or m does not divide u_k.

Thus Mollin and Walsh verified, with $m = 7$, that up to $k = 114, 254, 287$ the assertion (E_0') is satisfied.

Here are some related conjectures:

(E′) For every $k \geq 1$ let n_k be the powerful number distinct from and closest to 2^k; then $\lim_{n \to \infty} |n_k - 2^k| = \infty$.

(E″) There are at most finitely many integers $k \geq 1$, such that $2^k - 1$ or $2^k + 1$ is powerful.

(E‴) There are at most finitely many integers $k \geq 1$, such that $2^k - 1$ is powerful.

(E^{iv}) There are at most finitely many even integers $2k \geq 2$, such that $2^{2k} - 1$ is powerful.

Of course, (E′) $\Rightarrow$ (E″) $\Rightarrow$ (E‴) $\Rightarrow$ (E^{iv}).

Consider also the conjecture:

(*E**) There exists only finitely many triples of consecutive powerful numbers.

Then (E) $\Rightarrow$ (E*) $\Rightarrow$ (E^{iv}). Just note that if $2^{2k} - 1$ is powerful, then so are the consecutive integers $2^k - 1$, 2^k, 2^{k+1}.

Consider the statement:

(W) $\#\{p \text{ prime} \mid 2^{p-1} \not\equiv 1 \pmod{p^2}\} = \infty$

or equivalently, the set $\mathscr{W}_2^{(1)} \setminus \mathscr{W}_2^{(2)}$ is infinite. As already mentioned, this is heuristically true. Also, by Wieferich's theorem, (W) implies that the first case of FLT is true for infinitely many primes.

Granville has proved [4] that (E) implies (W), which provides a very interesting and surprising connection between powerful numbers and the first case of FLT. It will be shown below that, in fact, (E^{iv}) already implies (W)—but the proof is almost verbatim to Granville's. It is included here for the convenience of the reader, and to stress that only the weaker assumption (E^{iv}) suffices.

The lemma below was indicated by De Leon (in connection with a problem of Powell [10]):

LEMMA 1. *If p is an odd prime, $m \geqslant 2$, $p \mid 2^m - 1$, and $p^2 \mid 2^{p-1} - 1$ then $p^2 \mid 2^m - 1$.*

Proof. Let g be the order of 2 modulo p, so g divides $p-1$ and m. Then $2^g = 1 + ap$ and writing $p - 1 = gh$, $2^{p-1} \equiv 2^{gh} \equiv (1+ap)^h \equiv 1 + hap \pmod{p^2}$ so $p \mid a$, hence $2^g \equiv 1 \pmod{p^2}$ and finally, $2^m \equiv 1 \pmod{p^2}$. ∎

PROPOSITION 2. (E^{iv}) *implies* (W).

Proof. If (W) is false, then there exists p_0 such that if p is any prime, $p > p_0$, then $2^{p-1} \equiv 1 \pmod{p^2}$.

Let $t = \prod_{p \leqslant p_0} p$, so $\phi(t) = \prod_{p \leqslant p_0} (p-1)$.

For every $h \geqslant 1$ let $a_h = 2^{h t \phi(t)}$. Then $a_h - 1$ is a powerful number. Indeed, 2 does not divide $a_h - 1$. If p is a prime, $2 < p \leqslant p_0$, then $p(p-1)$ divides $t\phi(t)$, so from $2^{p(p-1)} \equiv 1 \pmod{p^2}$ then $2^{ht\phi(t)} \equiv 1 \pmod{p^2}$, i.e., $p^2 \mid a_h - 1$. Finally, if $p_0 < p$ and $p \mid a_h - 1$ then by the hypothesis and lemma, p^2 divides $a_h - 1$.

This contradicts (E^{iv}). ∎

The above conjectures (E″), (E‴) suggest the consideration of Fermat numbers, Mersenne numbers, and the well-known theorem of Bang and Zsigmondy:

If $a > b \geqslant 1$, $\gcd(a, b) = 1$, *then for every* $m \geqslant 1$ (*with the exception of* $a = 2$, $b = 1$, $m = 6$), *there exists a prime* p_m *which divides* $a^m - b^m$, *but does not divide* $a^h - b^h$, *for every* h dividing m, $h < m$).

p_m is called a *primitive* prime divisor of $a^m - b^m$, and p_m does not divide $a^h - b^h$, for every h, $1 \leqslant h < m$.

Consider the statement:

(B_2) There exist infinitely many $m>1$ such that 2^m-1 has a primitive prime divisor p_m for which p_m^2 does not divide 2^m-1.

LEMMA 2. (E''') *implies* (B_2).

Proof. Suppose that there exists m_0, such that for every $m>m_0$ and, for every primitive prime divisor p_m of 2^m-1, p_m^2 divides 2^m-1. Let q be a prime, $q>m_0$, let $n=q^s$, $s\geqslant 1$, and let l be a prime divisor of $2^{q^s}-1$; then l is a primitive prime divisor of $2^{q^h}-1$, for some h, $1\leqslant h\leqslant s$. Hence $l^2 \mid 2^{q^h}-1$, so also $l^2 \mid 2^{q^s}-1$. This shows that $2^{q^s}-1$ is powerful, for every $s\geqslant 1$, contrary to the hypothesis (E'''). ∎

Note that (B_2) $\Rightarrow$ (W) is precisely Lemma 1.

This shows that (E''') $\Rightarrow$ (W), which follows, of course, from Proposition 2.

Concerning Fermat and Mersenne numbers, the following conjectures were spelled out by Schinzel:

(F) There exist infinitely many squarefree Fermat numbers.

(M) There exist infinitely many squarefree Mersenne numbers.

Consider also the following weaker conjectures:

(F′) There exist infinitely many Fermat numbers which are not powerful.

(M′) There exist infinitely many Mersenne numbers which are not powerful.

LEMMA 3. (F') $\Rightarrow$ (B_2) *and* (M') $\Rightarrow$ (B_2).

Proof. For the first implication, it is enough to show: if the prime number p divides F_n, but $p^2 \nmid F_n$, then p is a primitive prime factor of $2^{2^{n+1}}-1$ and $p^2 \nmid 2^{2^{n+1}}-1$. It is clear that $p \nmid 2^{2^n}-1$ and $p \mid 2^{2^{n+1}}-1$, but $p^2 \nmid 2^{2^{n+1}}-1$. If p is not a primitive prime factor of $2^{2^{n+1}}-1$, then it is a primitive prime factor of $2^{2^e}-1$, with $1\leqslant e\leqslant n$. But $p \nmid 2^{2^{e-1}}+1=F_{e-1}$ (since Fermat numbers are pairwise relatively prime), hence $p \mid 2^{2^{e-1}}-1$, which is a contradiction.

Since every prime divisor of a Mersenne number is necessarily primitive, then (M') $\Rightarrow$ (B_2). ∎

Let

$$\mathscr{P}(M)=\{p \text{ prime} \mid p \text{ divides some Mersenne number}\},$$

$$\mathscr{P}^{(2)}(M)=\{p \text{ prime} \mid p^2 \text{ divides some Mersenne number}\},$$

$$\mathscr{P}(F) = \{p \text{ prime} \mid p \text{ divides some Fermat number}\},$$

$$\mathscr{P}^{(2)}(F) = \{p \text{ prime} \mid p^2 \text{ divides some Fermat number}\}.$$

The sets $\mathscr{P}(M)$, $\mathscr{P}(F)$ are infinite, because Mersenne numbers, as well as Fermat numbers, are pairwise relatively prime.

Rotkiewicz [16] and Warren and Bray [19] showed:

LEMMA 4. $\mathscr{P}(F) \cap \mathscr{W}_2^{(2)} = \mathscr{P}^{(2)}(F)$,

$$\mathscr{P}(M) \cap \mathscr{W}_2^{(2)} = \mathscr{P}^{(2)}(M).$$

It follows:

LEMMA 5. *If* $\mathscr{W}_2^{(2)}$ *is finite then* (F′) *and* (M′) *are true.*

Proof. If there exists n_0 such that for every $n > n_0$ the number F_n is powerful, since Fermat numbers are pairwise relatively prime, by Lemma 4, $\mathscr{W}_2^{(2)}$ is an infinite set, contrary to the hypothesis.

The proof is the same for (M′). ∎

It should be noted that, heuristically, $\mathscr{W}_2^{(2)}$ is an infinite set, so this lemma is likely uninteresting.

3. SOME REMARKS ABOUT CONJECTURE (E)

(E) implies:

(E_1) For every even integer $m \geqslant 2$, the number $m^4 - 1$ is not powerful, i.e., $m^2 + 1$ or $m^2 - 1$ is not powerful.

This statement, in turn implies:

(E_1^*) There exists only finitely many even integers $m \geqslant 2$ such that $m^4 - 1$ is powerful, i.e., $m^2 + 1$ and $m^2 - 1$ are powerful.

This suggests that one consider whether, *given* $a \geqslant 2$, it is possible to find even integers m such that $m^4 - 1$ is of the form a^2b^3 (with $b \geqslant 1$). This is, of course, a substantially weaker problem, but one which may be studied with the present methods.

PROPOSITION 3. *Let* $e \geqslant 1$. *Then, for every even integer* m, $m^{2^e+1} - 1$ *is not of the form* $a^h b^k$, *where* $k = 0$ *or* $k \geqslant 2$, $h \geqslant 2$, $b \geqslant 1$, $a \geqslant 1$ *and the number* $v(a)$ *of distinct prime factors of* a *is at most equal to* e.

Proof. First note that $m^{2^e+1} - 1 = c^f$ is impossible, with $f \geqslant 2$, $m \geqslant 1$, $c \geqslant 1$, $e \geqslant 1$. Indeed, $f \neq 2$; if $f = 3$ then by Euler's result, $m^{2^e+1} = 9$ so $e = 0$,

against the hypothesis. Finally, if $f \geqslant 4$ it is also impossible, by Chao Ko's result (C).

Thus $m^{2^{e+1}} - 1 = a^h b^k$ is impossible with $a = 1$ and $k \geqslant 2$, or with $k = 0$ and $h \geqslant 2$.

Let $k \geqslant 2$ and assume that there exists m even, $b \geqslant 1$, such that $m^{2^{e+1}} - 1 = a^h b^k$ where $a = p_1^{s_1} \cdots p_r^{s_r}$, $1 \leqslant r \leqslant e$, $s_i \geqslant 1$ (for $i = 1, ..., r$), and $p_1, ..., p_r$ are distinct primes. It will be shown, by induction on r, that this is impossible. Since m is even then $m^{2^e} - 1$, $m^{2^e} + 1$ are relatively prime. So

$$m^{2^e} - 1 = \left(\prod_{I \in I} p_i^{s_i} \right)^h b_1^k$$

$$m^{2^e} + 1 = \left(\prod_{j \in J} p_j^{s_j} \right)^h b_2^k,$$

where $\{1, 2, ..., r\} = I \cup J$, $I \cap J = \varnothing$, $\gcd(b_1, b_2) = 1$, $p_i \nmid b_2$ for every $i \in I$, $p_j \nmid b_1$ for every $j \in J$.

If $J = \varnothing$ then $m^{2^e} + 1 = b_2^k$ $(k \geqslant 2)$, which is impossible, by Lebesgue's result (B). If $J \neq \varnothing$, then $0 \leqslant \#(I) < r$, $\#(I) \leqslant e - 1$, and by induction, the first equation is impossible.

In particular, for every even integer m, the number $m^{2^{e+1}} - 1$ is not of the form $a^2 b^3$, with $b \geqslant 1$, and $v(a) \leqslant e$. ∎

The above proposition may be extended, as will be indicated.

Let C_1 be the Tijdeman constant, associated with Catalan's equation (see (F)). Let q be an odd prime, and for every $i \geqslant 2$, let $f_i(X)$ be the cyclotomic polynomial associated with q^i; let C_i be the constant indicated in (I).

PROPOSITION 4. *Let $e \geqslant 1$, let q be an odd prime, and $m_0 = \max\{C_1, C_2, ..., C_{e+1}\}$. If $m > m_0$ and $m \not\equiv 1 \pmod q$ then $m^{q^{e+1}} - 1$ is not of the form $a^h b^k$, where $k \geqslant 2$ or $k = 0$, $h \geqslant 2$, $b \geqslant 1$, $a \geqslant 1$, and $v(a) \leqslant e$.*

Proof. The proof is similar to that of the preceding proposition.

If $k = 0$ the equality $m^{q^{e+1}} - 1 = a^h$ is not possible, when $m \geqslant m_0 \geqslant C_1$.

Let $k \geqslant 2$ and assume that $m^{q^{e+1}} - 1 = a^h b^k$ with $h \geqslant 2$, $b \geqslant 1$, $0 \leqslant v(a) \leqslant e$. If $v(a) = 0$, the above relation is impossible, because $m > C_1$. Let $a = \prod_{i=1}^r p_i^{s_i}$, where $p_1, ..., p_r$ are distinct primes, $s_i \leqslant 1$ $(i = 1, ..., r)$, $1 \leqslant r = v(a) \leqslant e$. If $f_i(X)$ is the cyclotomic polynomial associated with q^i, then $m^{q^{e+1}} - 1 = (m^{q^e} - 1) f_{e+1}(m)$. Since $m \not\equiv 1 \pmod q$, then $\gcd(m^{q^e} - 1, f_{e+1}(m)) = \gcd(m^{q^e} - 1, q) = 1$. Hence

$$m^{q^e} - 1 = \left(\prod_{i \in I} p_i^{s_i} \right)^h b_1^k$$

$$f_{e+1}(m) = \left(\prod_{j \in J} p_j^{s_j} \right)^h b_2^k,$$

where $\{1, 2, ..., r\} = I \cup J$, $I \cap J = \emptyset$, $\gcd(b_1, b_2) = 1$, $p_i \nmid b_2$ for every $i \in I$, $p_j \nmid b_1$ for every $j \in J$.

If $J = \emptyset$ then $f_{e+1}(m) = b_2^k$ $(k \geqslant 2)$, which is impossible, since $m > m_0 \geqslant C_{e+1}$. If $J \neq \emptyset$ then $0 \leqslant \#(I) < r$, so $\#(I) \leqslant e - 1$. By induction, the first relation is impossible, because $m > m_0 \geqslant \max\{C_1, C_2, ..., C_e\}$. ∎

It is possible to obtain a better result when $h = 2$, $k = 3$, taking into account the results of Nagell (D) and Ljunggren (E).

The same proof yields:

PROPOSITION 5. *Let $e \geqslant 1$, let q be an odd prime, $q \not\equiv -1 \pmod 6$. Then, for every m, $m \not\equiv 1 \pmod q$, the number $m^{q^{e+1}} - 1$ is not of the form $a^2 b^3$, with $b \geqslant 1$ and $v(a) \leqslant e$.*

Now, the possibility of $m^{2^{e+1}} - 1 = a^2 b^3$ when $e < v(a)$ will be discussed; more specifically, the equations $X^2 - 1 = a^2 Y^3$ or even $X^2 - 1 = a^h Y^k$ with $a \geqslant 2$, $h \geqslant 2$, $k \geqslant 3$.

PROPOSITION 6. *Let $a \geqslant 2$, $h \geqslant 2$ be given.*

(1) *There exists $C > 0$ such that if $k > C$ then for every $m \geqslant 1$, $m^2 - 1$ is not of the form $a^h b^k$, with $b \geqslant 2$.*

(2) *There exists $C' > 0$ such that if $m \geqslant 1$, $b \geqslant 1$, $k \geqslant 3$, and $m^2 - 1 = a^h b^k$, then $m, b, k < C'$.*

Proof. (1) Consider the polynomial $f(X) = (1/a^h)(X^2 - 1)$. The assertion follows at once, applying the theorem of Schinzel and Tijdeman, quoted in (G).

(2) This follows similarly from (H) and Chao Ko's result. ∎

It should be noted here that, despite the above result, given $b \geqslant 2$ there exist infinitely many integers $m \geqslant 1$, $a \geqslant 1$, such that $m^2 - 1 = a^2 b^3$. Indeed, consider the real quadratic field $\mathbb{Q}(\sqrt{b})$ and let $x + y\sqrt{b}$ be a fundamental unit, with $x \geqslant 1$, $y \geqslant 1$. Then, for every $i \geqslant 1$, $(x + y\sqrt{b})^{ib} = c_i + d_i b\sqrt{b}$, with positive integers c_i, d_i, so $c_i^2 - d_i^2 b^3 = 1$, thus $c_i^2 - 1 = d_i^2 b^3$, with $c_i, d_i \geqslant 1$. Note that this situation is not ruled out by the results of Schinzel and Tijdeman. Also, if b is even then each c_i is odd. If b is odd and d_i is even, c_i is again odd; finally, if b and d_i are both odd, then c_i would be even, however, this case contradicts the conjecture (E_0), as formulated by Mollin and Walsh.

The final result concerns the family of equations

$$E_h: X^2 - 1 = a^h y^k,$$

where $a \geqslant 2$, $k \geqslant 3$ are given and the parameter $h \geqslant 2$.

For every $h \geqslant 2$, let $Z_h = \{(m, b) \mid m \geqslant 1,\ b \geqslant 1,\ m^2 - 1 = a^h b^k\}$.

By (H), Z_h is finite (and even effectively computable). Let $B_h = \max\{b \mid (m, b) \in Z_h\}$.

LEMMA 6. *Let $a \geqslant 2$, $k \geqslant 3$. For every $h \geqslant 2$ there exists $e \geqslant 1$ (depending on a, k, h) such that if $h' = 1 + fk$, $f \geqslant e$, then $Z_{h'h} = \varnothing$.*

Proof. Let $f \geqslant 1$, $h' = 1 + fk$. If $(m, b) \in Z_{h'h}$ then $m^2 - 1 = a^{h'h} b^k = a^h (a^{hf} b)^k$, so $(m, a^{hf} b) \in Z_h$.

Taking e such that $a^e > B_h$ and $f \geqslant e$ then $Z_{h'h} = \varnothing$, otherwise $a^e \leqslant a^{hf} b \leqslant B_h < a^e$, which is absurd. ∎

For every $N \geqslant 2$, let

$$D_N = \{h \mid 2 \leqslant h \leqslant N,\ Z_h = \varnothing\}.$$

PROPOSITION 7. *If $a \geqslant 2$, $k \geqslant 3$ then* $\liminf_{N \to \infty} (\#(D_N)/N) \geqslant 1/k$.

Proof. Note, to begin, that for every $N \geqslant 1$ there exists m such that $mk \leqslant N < (m+1)k$; hence

$$\frac{m}{m+1} \cdot \frac{\#(D_{mk})}{mk} < \frac{\#(D_N)}{N}.$$

Thus, it suffices to show that for every $\varepsilon > 0$ there exists $m_0 \geqslant 1$ such that if $m \geqslant m_0$ then $\#(D_{mk})/mk > (1/k) - \varepsilon$.

Let $t \geqslant 1$ be arbitrary, and let $p_1 < p_2 < \cdots < p_t$ be the smallest t prime numbers such that $p_i \equiv 1 \pmod{k}$. Let $P_t = \prod_{i=1}^{t} p_i$.

For every p_i, consider the equation E_{p_i}, let $e_i \geqslant 1$ be the smallest integer such that $a^{e_i} > B_{p_i}$, and let $p_i' = 1 + e_i k$.

Let $K = K_t = p_t \max\{p_1', \ldots, p_t'\}$ and let m be such that $m > K$. Define

$$S = S_{t,m} = \{2 \leqslant h \leqslant mk \mid \text{there exists } i,\ 1 \leqslant i \leqslant t, \text{ such that } h = p_i h_i \text{ with } h_i \equiv 1 \pmod{k}\},$$

$$S' = S'_{t,m} = \{h \in S \mid K < h\}.$$

Then $S \subseteq S' \cup \{1, 2, \ldots, K\}$; note also that if $h \in S$ then $h \equiv 1 \pmod{k}$.

Moreover, $S' \subseteq D_{mk}$ because if $h \in S'$ then $h = p_i h_i > K \geqslant p_i p_i'$, so $h_i > p_i'$. By Lemma 6, $Z_h = Z_{p_i h_i} = \varnothing$, thus $h \in D_{mk}$.

Then $\#(D_{mk}) \geqslant \#(S') \geqslant \#(S) - K$.

In order to find a lower bound for $\#(S)$, first note that if p is a prime, $p \equiv 1 \pmod{k}$, if x is such that $(1 + xk)\, p \leqslant mk < (1 + (x+1)k)\, p$ then $x \leqslant ((mk/p) - 1)/k = m/p - 1/k < x + 1$, so $x > (m/p) - (1/k) - 1$. Similarly, if $p - p'$ are distinct primes, $p \equiv p' \equiv 1 \pmod{k}$, if y is such that $(1 + yk)\, pp' \leqslant mk < (1 + (y+1)k)\, pp'$ then $y \leqslant ((mk)/(pp') - 1)/k < y + 1$, so $y \leqslant (m/pp') - (1/k)$.

Proceeding in the same way,

$$\#(S) \geqslant \sum_p \left(\frac{m}{p} - \frac{1}{k} - 1\right) - \sum_{p\,p'} \left(\frac{m}{pp'} - \frac{1}{k}\right) + \sum_{p,\,p',\,p''} \left(\frac{m}{pp'p''} - \frac{1}{k} - 1\right) - \cdots,$$

where the sums are for distinct primes $p, p', p'', \ldots$ belonging to the set $\{p_1, p_2, \ldots, p_t\}$. Using the Möbius function, the above sum may be rewritten as

$$\begin{aligned} &- \sum_{1 \neq d \mid P_t} \frac{m}{d}\mu(d) - \frac{1}{k}\left[\binom{t}{1} - \binom{t}{2} + \binom{t}{3} - \cdots\right] \\ &\quad - \left[\binom{t}{1} + \binom{t}{3} + \cdots\right] \\ &= m - \sum_{d \mid P_t} \frac{m}{d}\mu(d) - \frac{1}{k} - 2^{t-1} \\ &= \left(1 - \sum_{d \mid p} \frac{\mu(d)}{d}\right) - \frac{1}{k} - 2^{t-1} \\ &= m\left[1 - \prod_{i=1}^{t}\left(1 - \frac{1}{p_i}\right)\right] - \frac{1}{k} - 2^{t-1}. \end{aligned}$$

According to Dirichlet's theorem, $\sum_{p \equiv 1 \,(\mathrm{mod}\, k)} (1/p)$ is divergent, hence $\prod_{p \equiv 1 \,(\mathrm{mod}\, k)} (1 - (1/p))$ tends to 0.

So, given $\varepsilon > 0$ there exists t such that $\prod_{i=1}^{t} (1 - (1/p_i)) < k\varepsilon/2$. Let m_0 be such that $m_0 > K = K_t$ and $((1/k) + 2^{t-1} + k)/m_0 < k\varepsilon/2$.

If $m \geqslant m_0$ then $\#(D_{mk})/mk > (1 - (k\varepsilon)/2)/k - \varepsilon/2 = 1/k - \varepsilon$, completing the proof. ∎

To conclude, I shall indicate some open questions.

(a) Do there exist only finitely many even powerful numbers m such that $m^2 - 1$ is powerful?

(b) Do there exist only finitely many even integers m such that $m^4 - 1$ is powerful?

(c) Is it true that

$$\lim_{M \to \infty} \frac{\#\{m \mid 2 \leqslant m \leqslant 2M,\ m \text{ is even},\ m^4 - 1 \text{ is not powerful}\}}{M} = 1?$$

(d) Is it true that

$\lim_{n\to\infty} 1/M \#\{m \mid 2 \leqslant m \leqslant 2M,\ m \text{ is even and there exists } e \geqslant 1 \text{ such that } m^{2^e+1} - 1 \text{ is not powerful}\} = 1$?

A positive answer to any of the above questions implies that the successive answers are also affirmative.

Let $a \geqslant 2$ be given. Does there exist an effectively computable constant $C > 0$, such that if $x, y \geqslant 1$, $u, v \geqslant 2$, and $ax^u - y^v = 1$, then $x, y, u, v < C$?

Does there exist an effectively computable constant $C > 0$, such that if $x, y, z > 1$, $t \geqslant 2$, and $z^t + 1 = x^2y^3$, then $x, y, z, t < C$?

REFERENCES

1. L. M. ADLEMAN AND D. R. HEATH-BROWN, The first case of Fermat's last theorem, *Invent. Math.* **79** (1985), 409–416.
2. P. ERDÖS, Problems and results on consecutive integers, *Eureka* **38** (1975/6), 3–8.
3. E. FOUVRY, Théorème de Brun–Titchmarsh: Application au théorème de Fermat, *Invent. Math.* **79** (1985), 383–407.
4. A. GRANVILLE, Powerful numbers and Fermat's last theorem, *C. R. Math. Rep. Acad. Sci. Canada* **8** (1986), 215–218.
5. A. GRANVILLE AND M. B. MONAGAN, The first case of Fermat's last theorem is true for all prime exponents up to 714, 591, 416, 091, 389, preprint, Queen's University.
6. N. G. GUNDERSON, Derivation of criteria for the first case of Fermat's last theorem and the combination of these criteria to produce a new lower bound for the exponent, Thesis, Cornell University, 1948.
7. W. LJUNGGREN, Some theorems on the indeterminate equation $(x^n - 1)/(x - 1) = y^q$ (in Norwegian), *Norske Mat. Tidsskrift* **25** (1943), 17–20.
8. R. A. MOLLIN AND P. G. WALSH, On powerful numbers, *Internat. J. Math. Math. Sci.* **9** (1986), 801–806.
9. T. NAGELL, Des équations indéterminées $x^2 + x + 1 = y^n$ et $x^2 + x + 1 = 3y^n$, *Norske Mat. Forenings Skrifter Ser. I*, No. 2 (1921).
10. B. POWELL AND M. J. DE LEON, Problem E2631 (and its solution), *Amer. Math. Monthly* **84** (1977), 57; **87** (1978), 279–280.
11. S. PUCCIONI, Un teorema per una resoluzione parziale del famoso teorema di Fermat, *Archimede* **20** (1968), 219–220.
12. P. RIBENBOIM, "13 Lectures on Fermat's Last Theorem," Springer-Verlag, Berlin/New York, 1979.
13. P. RIBENBOIM, Consecutive powers, *Expo. Math.* **2** (1984), 193–221.
14. P. RIBENBOIM, "The Book of Prime Number Records," Springer-Verlag, Berlin/New York, 1988.
15. P. RIBENBOIM, Impuissants devant les puissances, *Expo. Math.* **6** (1988), 3–28.
16. A. ROTKIEWICZ, Sur les nombres de Mersenne dépourvus de diviseurs carrés et sur les nombres naturels n tels que $n^2 \mid 2^n - 2$, *Matem. Vecnik* (2) **17** (1965), 78–80.
17. A. SCHINZEL AND R. TIJDEMAN, On the equation $y^m = P(x)$, *Acta Arithm.* **31** (1976), 194–204.
18. R. TIJDEMAN, On the equation of Catalan, *Acta. Arithm.* **29** (1976), 197–209.
19. L. J. WARREN AND H. BRAY, On the square-freeness of Fermat and Mersenne numbers, *Pacific J. Math.* **22** (1967), 563–564.